

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-264178

(43)Date of publication of application : 13.10.1995

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

G06F 13/00

G06F 15/00

H04L 12/40

(21)Application number : 06-052212

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 23.03.1994

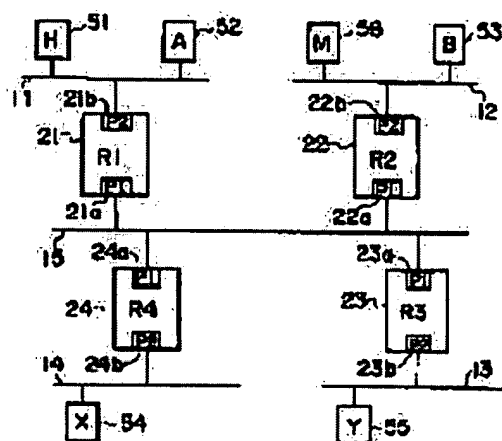
(72)Inventor : ITAGAKI KANJI

(54) SECURITY SYSTEM

(57)Abstract:

PURPOSE: To obtain the security system in which illegal access is inhibited and an address accessed illegally is located.

CONSTITUTION: The system is provided with repeaters 21-24 informing alarm information when illegal access takes place to terminal equipments 51-55 on LANs 11-14 connecting to a concerned repeater from any of the terminal equipments 51-55 and a management equipment 56 displaying the content when alarm information is received. The management equipment 56 retrieves to which port of each of the repeaters 21-24 the terminal equipment making illegal access is connected based on the alarm information and the access history information having each of the repeaters 21-24 to locate to which LAN the terminal equipment is connected.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-264178

(43) 公開日 平成7年(1995)10月13日

(51) Int.Cl.⁹

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

9/10

9/12

H 0 4 L 9/00

Z

11/00

320

審査請求 未請求 請求項の数8 OL (全9頁) 最終頁に続く

(21) 出願番号

特願平6-52212

(22) 出願日

平成6年(1994)3月23日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 板垣 寛二

神奈川県鎌倉市上町屋325番地 三菱電機

株式会社コンピュータ製作所内

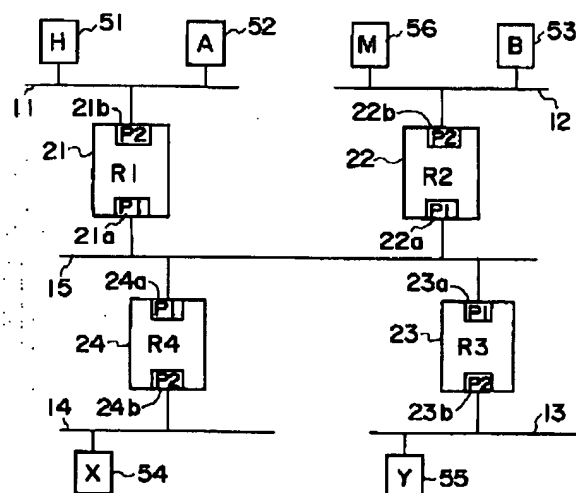
(74) 代理人 弁理士 吉田 研二 (外2名)

(54) 【発明の名称】 セキュリティ方式

(57) 【要約】

【目的】 不正アクセスを禁止するのみならず不正アクセスをした箇所を特定することのできるセキュリティ方式を提供する。

【構成】 いずれかの端末装置51～55から自中継装置に接続されたLAN11～14上の端末装置51～55に対して不正アクセスがあった場合、アラーム情報を通知する中継装置21～24と、アラーム情報を受信するとその内容を表示する管理装置56と、を有するネットワークシステムにおいて、管理装置56は、アラーム情報と各中継装置21～24が有するアクセス履歴情報とから不正アクセスをした端末装置が各中継装置21～24のどちら側のポートに接続されているかを絞り込んでいくことで、どのLAN上に接続されているかを特定する。



【特許請求の範囲】

【請求項1】 固有のアドレスが割り付けられた端末装置を接続する伝送媒体と、
前記伝送媒体を介して前記端末装置間の通信を中継する中継装置と、

いずれかの前記伝送媒体に接続されネットワークシステムを管理する管理装置と、
を有し、許可された各端末装置間の通信を行わせるセキュリティ方式において、

前記中継装置は、自中継装置に接続されている前記伝送媒体上の前記端末装置に対する不正アクセスまたは障害を検出すると、アラーム情報を前記管理装置に通知することを特徴とするセキュリティ方式。

【請求項2】 請求項1記載のセキュリティ方式において、

前記中継装置は、前記アラーム情報を通知する条件を登録するアラーム通知条件登録手段を有することを特徴とするセキュリティ方式。

【請求項3】 請求項1記載のセキュリティ方式において、

前記管理装置は、受信したアラーム情報を表示する手段を有することを特徴とするセキュリティ方式。

【請求項4】 請求項1記載のセキュリティ方式において、

前記管理装置は、任意の前記中継装置に対し、自中継装置に接続されている前記伝送媒体を介してのアクセス状況を記録したアクセス履歴情報の送信を要求する手段を有することを特徴とするセキュリティ方式。

【請求項5】 請求項4記載のセキュリティ方式において、

前記管理装置は、前記中継装置から受信した前記アクセス履歴情報と前記アラーム情報とから不正アクセスをした前記端末装置が接続されている前記伝送媒体を特定する手段を有することを特徴とするセキュリティ方式。

【請求項6】 請求項4記載のセキュリティ方式において、

前記管理装置は、前記中継装置から受信した前記アラーム情報から前記端末装置を特定する手段を有することを特徴とするセキュリティ方式。

【請求項7】 請求項1及び請求項3乃至請求項6記載のセキュリティ方式において、

前記各管理装置は、前記端末装置により実現することを特徴とするセキュリティ方式。

【請求項8】 請求項1記載のセキュリティ方式において、

前記中継装置は、設定されている許可／禁止情報に基づき受信したフレームの中継制御の許可／禁止の判断を行い、中継制御を禁止すると判断した場合において設定されているアラーム情報通知条件に基づき不正アクセスまたは障害を検出することを特徴とするセキュリティ方

式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、セキュリティ方式、特に複数のローカルエリアネットワーク（以下、LANという）あるいは公衆網等の伝送媒体により構築されるネットワークシステムにおいて、禁止された端末装置に不正にアクセスをしようとした端末装置を突き止めるセキュリティ方式に関する。

【0002】

【従来の技術】従来からブリッジ、ルータ等の中継装置を介して複数のLANを接続して構築するネットワークシステムにおいて、異なるLANに接続された端末装置間の通信不可等のアクセス制御を行うために各種セキュリティ方式が採用されている。

【0003】例えば、特開平3-280639号公報には、各種テーブルを用いて許可されていない端末装置からの不正アクセスを禁止する方式が記載されている。図8は、この特開平3-280639号公報に開示された従来のローカルエリアネットワークシステムの構成図である。

【0004】幹線LAN1と各支線LAN2-1～2-4は、それぞれアドレスNA1～NA4が割り当てられたノード装置N21～N24で接続されている。支線LAN2-1～2-4のいずれかには固有のアドレスTA1～TA5が割り当てられた端末装置Tが、また支線LAN2-1にはアドレスNMAが割り当てられたネットワーク管理局NMSが、それぞれ接続されている。また、ノード装置N21、N22はグループ番号G1のグループ、ノード装置N23、N24グループ番号G2のグループとしてグループ化されている。

【0005】各ノード装置N21～N24は、自ノード装置に接続された支線LAN2-1～2-4に接続された端末装置TのアドレスTA1～TA5を登録する支線側フィルタリングテーブルTBS1～TBS4と、自ノード装置に接続されていない、すなわち自ノード装置から見て幹線LAN1側に接続された端末装置TのアドレスTA1～TA5を登録する幹線側フィルタリングテーブルTBK1～TBK4と、特権端末装置のアドレスを登録する特権端末テーブルTTB1～TTB4と、ネットワーク管理局NMSのアドレスNMAを登録するNMSアドレステーブルNTB1～NTB4と、をそれぞれ有している。

【0006】次に、この従来例において、アドレスTA3の端末装置T（以下、端末装置T（TA3）と記す）からアクセスが許可されていない端末装置T（TA4）に対してフレームを送信する場合の動作を説明する。なお、通信に使用されるフレームには、宛先アドレス、発信元アドレスが含まれている。

【0007】ノード装置N22は、端末装置T（TA

3) からフレームを受信すると、自支線LAN2-2に端末装置T(TA4)が接続されていないことから明らかなように、支線側フィルタリングテーブルTBS2に宛先となる端末装置T(TA4)のアドレスTA4が登録されていないので、フレームにグループ番号G1をのせて幹線LAN1に転送する。

【0008】ノード装置N23は、幹線LAN1から受信した当該フレームには自ノード装置と異なるグループ番号が書き込まれていることを確認した後、以下の手順で処理を行う。

【0009】まず、当該フレームの宛先アドレスの内容をNMSアドレステーブルNTB3の中から検索する。発信元となる端末装置T(TA3)のアドレスTA3は登録されていないので、次に当該フレームの発信元アドレスの内容を特権端末テーブルTTB3の中から検索する。端末装置T(TA3)のアドレスTA3は登録されていないので、次に当該フレームの発信元アドレスの内容をNMSアドレステーブルNTB3の中から検索する。端末装置T(TA3)のアドレスTA3は登録されていないので、その結果、当該フレームは廃棄される。

【0010】このようにして、従来例におけるノード装置N21~N24は、アクセスが許可されていない端末装置Tからのフレームを廃棄することで不正アクセスを禁止していた。

【0011】

【発明が解決しようとする課題】しかしながら、従来においては、上記のようにフレームを廃棄することで不正アクセスを禁止することはできても不正にアクセスしようとした事実を知ることはできない。従って、どの端末装置から不正にアクセスしようとしたということを知ることはできない。

【0012】本発明は以上のような問題を解決するためになされたものであり、その目的は、不正アクセスを禁止するのみならず不正アクセスをした箇所を特定することのできるセキュリティ方式を提供することにある。

【0013】

【課題を解決するための手段】以上のような目的を達成するために、請求項1記載の発明は、固有のアドレスが割り付けられた端末装置を接続する伝送媒体と、前記伝送媒体を介して前記端末装置間の通信を中継する中継装置と、いずれかの前記伝送媒体に接続されネットワークシステムを管理する管理装置と、を有し、許可された各端末装置間のみの通信を行わせるセキュリティ方式において、前記中継装置は、自中継装置に接続されている前記伝送媒体上の前記端末装置に対する不正アクセスまたは障害を検出すると、アラーム情報を前記管理装置に通知することを特徴とする。

【0014】請求項2記載の発明は、請求項1記載のセキュリティ方式において、前記中継装置は、前記アラーム情報を通知する条件を登録するアラーム通知条件登録

手段を有することを特徴とする。

【0015】請求項3記載の発明は、請求項1記載のセキュリティ方式において、前記管理装置は、受信したアラーム情報を表示する手段を有することを特徴とする。

【0016】請求項4記載の発明は、請求項1記載のセキュリティ方式において、前記管理装置は、任意の前記中継装置に対し、自中継装置に接続されている前記伝送媒体を介してのアクセス状況を記録したアクセス履歴情報の送信を要求する手段を有することを特徴とする。

10 【0017】請求項5記載の発明は、請求項4記載のセキュリティ方式において、前記管理装置は、前記中継装置から受信した前記アクセス履歴情報と前記アラーム情報とから不正アクセスをした前記端末装置が接続されている前記伝送媒体を特定する手段を有することを特徴とする。

【0018】請求項6記載の発明は、請求項4記載のセキュリティ方式において、前記管理装置は、前記中継装置から受信した前記アラーム情報から前記端末装置を特定する手段を有することを特徴とする。

20 【0019】請求項7記載の発明は、請求項1及び請求項3乃至請求項6記載のセキュリティ方式において、前記各管理装置は、端末装置により実現することを特徴とする。

【0020】請求項8記載の発明は、請求項1記載のセキュリティ方式において、前記中継装置は、設定されている許可/禁止情報に基づき受信したフレームの中継制御の許可/禁止の判断を行い、中継制御を禁止すると判断した場合において設定されているアラーム情報通知条件に基づき不正アクセスまたは障害を検出することを特徴とする。

【0021】

【作用】以上のような構成を有する本発明に係るセキュリティ方式においては、中継装置は不正アクセスを検出すると、アラーム情報を管理装置に通知するので、管理装置は、不正アクセスがあったことを検出することができ、その内容を表示することでネットワーク管理者等に知らせることができる。

【0022】アラーム通知条件登録手段は、アラーム情報を管理装置に通知する条件を設定登録することができる。

【0023】管理装置は、任意の中継装置に対しアクセス履歴情報の送信を要求し、その結果得られたアクセス履歴情報とアラーム情報とから不正アクセスをした前記端末装置が接続されている伝送媒体を特定することができる。

【0024】また、管理装置は、任意の中継装置に対しアクセス履歴情報の送信を要求し、その結果得られたアラーム情報から不正アクセスをした前記端末装置を特定することができる。

50 【0025】また、中継装置は、設定されている許可/

禁止情報に基づき受信したフレームの中継制御の許可／禁止の判断を行う。その結果、中継制御を禁止すると判断した場合、設定されているアラーム情報通知条件に基づいて、アラーム通知の必要性があるかどうかを判断する。必要性があると判断することにより不正アクセスまたは障害を検出するとし、アラーム情報を管理装置に通知する。従って、管理装置は、不正アクセスがあったことを検出することができる。

【0026】

【実施例】以下、図面に基づいて、本発明の好適な実施例を説明する。

【0027】図1は、本実施例におけるセキュリティ方式が実施されるネットワークシステムの構成図である。

【0028】伝送媒体であるLAN11、12、13、14、15は、それぞれ中継装置21、22、23、24で接続されている。各LAN11、12、13、14、15のいずれかには、それぞれに固有のアドレスが割り当てられた端末装置51、52、53、54、55が接続されており、各端末装置51～55は、物理的に各LAN11～15、中継装置21～24を介して通信可能である。また、LAN12には、端末装置であってネットワークシステム全体を管理する管理装置56が接続されている。各中継装置21～24は、LAN11～15を物理的に接続するポートを有している。もちろん、3つ以上のポートを有してもよいが、図に示したように本実施例における各中継装置21～24は、それぞれ2本のLANを接続しているためそれぞれ2つのポート番号P1、P2のポート21a、21b、22a、22b、23a、24a、24bを有している。

【0029】図2は、中継装置21の構成を示した図である。中継装置21は、前述したポート21a、21bと、中継装置21における処理を制御する制御部21cと、中継を許可／禁止する端末装置に関する情報が登録されている中継制御テーブル21dと、を有する。この中継制御テーブル21dに登録する情報としては、特権端末装置のアドレス、管理装置56のアドレス等がある。更に、本実施例における中継装置21は、不正アクセスまたは障害があったときなどに管理装置56にアラーム情報をポートを介して通知するアクセス情報通知部21eと、管理装置56にアラーム情報を通知すべき条件を登録するアラーム情報通知条件登録部21fと、を有することを特徴とする。これにより、不正アクセス等があったことを管理装置56に通知することができる。更に、また本実施例における中継装置21は、自中継装置21に接続されているLAN11、15を介してのアクセス状況、すなわちどの端末装置からどの端末装置へのアクセス要求があったかのアクセス履歴を記録するアクセス履歴情報記憶部21gを有することを特徴とする。図3は、中継装置21～24それぞれが有しているアクセス履歴情報であり、端末装置間通信で使用される

フレームを受信した側のポート番号とフレームの発信元となる端末装置のアドレスとが対応づけられて記録される。これにより、フレームの発信元となる端末装置が中継装置21～24のどちら側のLANに存在するかを知ることができる。他の中継装置22、23、24も同様の構成である。なお、本実施例における端末装置間通信に使用されるフレームには、少なくとも発信元アドレスと宛先アドレスとが含まれている必要がある。

【0030】図4は、管理装置56の構成を示した図である。管理装置56は、LAN12を介して他の装置との間でフレーム等の送受信を行う入出力部56aと、本装置における処理を制御する制御部56bと、メモリ56cと、を有する。更に、本実施例における管理装置56は、中継装置21～24から受信したアラーム情報を表示するアラーム情報表示部56dを有することを特徴としており、これにより、いずれかの端末装置への不正アクセスがあったという事実を即座にシステム管理者等に知らせることができる。更に、また本実施例における管理装置56は、任意の中継装置21～24に対して各中継装置21～24が記憶しているアクセス履歴情報の送信を要求しうるアクセス履歴情報送信要求部56eを有することを特徴としており、これにより、管理装置56において、どの端末装置51～55が中継装置21～24のどちら側に存在しているかを知ることができる。

【0031】図5は、本実施例における中継装置21～24の処理を示したフローチャートであり、以下、これに基づいて本実施例における中継装置21～24の動作について説明する。

【0032】例として端末装置54から端末装置51にフレームを送信（アクセス）する場合を説明する。

【0033】まず、各中継装置21～24の中継制御テーブル21dに何も設定されていない場合について説明する。

【0034】中継装置24は、端末装置54からフレームをLAN14、ポート24bを介して受信すると、アクセス履歴情報記憶部21gに端末装置54のアドレス（X_addr）と受信したポート番号P2を対応づけて記憶（保存）する（ステップ101）。なお、ポート24a、24bに接続されているLAN14、15上の端末装置は、予めアクセス履歴情報記憶部21gに設定しておいてもよい。ここで、中継制御テーブル21dに設定があるかを判断する（ステップ102）。この場合、設定がないので、次に、フレーム受信したポート番号は、アクセス履歴情報において端末装置51のアドレス（H_addr）は、端末装置54と同じポート番号であるかを比較参照する（ステップ103）。仮に、端末装置51が端末装置54と同じポート番号P2であれば、端末装置51は同一のLAN14上にあると判断され、そのフレームを他のLAN上に送出する必要はない。従って、当該フレームを廃棄する（ステップ108）。ま

た、端末装置51が端末装置54と同じポート番号P2でなければ、そのポートからフレームを送出する(ステップ109)。本実施例においては、ポート番号P1からフレームを送出する。なお、端末装置51のアドレスがまだ記憶されていなければ、当該フレームを受信したポート以外のポート24aから送出的(ステップ109)。ポート24aから送出的されたフレームは、LAN15に接続されている中継装置21、22、23により受信される。フレームを受信すると、各中継装置21、22、23におけるアクセス履歴情報記憶部21gに端末装置54のアドレス(X__a d r)と受信したポート番号P1を対応づけて記憶する(ステップ101)。ここで、各中継装置21、22、23において、フレーム内の宛先アドレス(この例においてはH__a d r)を参照し、自アクセス履歴情報記憶部21gに宛先アドレスと受信したポート以外のポート番号(本実施例においてはP2のみ)とで対応づけられたアクセス履歴情報があるかを検索する。この例においては、中継装置21のアクセス履歴情報記憶部21gに記録されているので、中継装置21のみがポート21bからフレームを送出する。他の中継装置22、23は、当該フレームを廃棄する。

【0035】このようにして、各中継装置21~24の中継制御テーブル21dに何も設定されていない場合、端末装置51は、LAN11を介して端末装置54から送出的されたフレームを受信することができる。

【0036】次に、中継装置21の中継制御テーブル21dに端末装置への許可/禁止情報が設定登録されている場合について説明する。本実施例においては、以下の許可/禁止情報(1)及び(2)が設定されているものとする。

【0037】(1) 端末装置51と端末装置53との間の双方向のフレームの中継を許可する。

【0038】(2) LAN13、14に接続されている端末装置からのフレームの中継を禁止する。

【0039】また、中継装置21のアラーム情報条件登録部21fに、LAN13、14に接続されている端末装置からフレームを受信した場合、アラーム情報を通知するという条件を登録しておく。

【0040】このように設定された場合であっても、端末装置51、52、53間でのフレーム送受信、すなわちアクセスは可能である。また、端末装置53、54、55間のアクセスも可能である。

【0041】ここで、上記と同様、端末装置54から端末装置51にフレームを送信(アクセス)する場合について説明するが、主要でない上記と同様の動作についての説明は省略する。

【0042】端末装置54がフレームを送出すると、中継装置24は、端末装置54からフレームをLAN14、ポート24bを介して受信し、アクセス履歴情報

憶部21gに端末装置54のアドレス(X__a d r)と受信したポート番号P2を対応づけて記憶(保存)する(ステップ101)。ここで、中継装置24の中継制御テーブル21dには何も設定されていないので(ステップ102)、上記と同様、ポート番号P1から当該フレームを送出する(ステップ109)。

【0043】中継装置21は、中継装置24からのフレームを受信すると、アクセス履歴情報記憶部21gに端末装置54のアドレス(X__a d r)と受信したポート番号P1を対応づけて記憶する(ステップ101)。ここで、中継制御テーブル21dに設定があるかを判断する(ステップ102)。この場合、設定があるので、次に、中継制御が許可されているかを判断する(ステップ104)。前述したとおり、中継装置21の中継制御テーブル21dには前述したとおり許可/禁止情報

(1)、(2)が設定されているので、許可された中継制御は、端末装置51と端末装置53との間の双方向のフレームの中継のみである。次に、中継制御が禁止されているかを判断する(ステップ105)。前述したとおり、この例のLAN14に接続されている端末装置24からのフレームの中継は禁止されているので、次にアラーム情報通知部21eにおいてアラーム通知の必要性を判断する(ステップ106)。前述したように、中継装置21のアラーム情報条件登録部21fには、LAN14に接続されている端末装置54からフレームを受信した場合、アラーム情報を通知するという条件が登録されているので、アラーム情報通知部21eは、ポート21aからアラーム情報を管理装置56に通知する(ステップ107)。この通知されるアラーム情報には、アラーム情報送元となる中継装置を特定できるアドレス等の情報、フレームの発信元、宛先となる端末装置のアドレス等が含まれている。中継装置21は、アラーム情報通知後、当該フレームを廃棄する(ステップ108)。

【0044】以上のようにして、不正アクセスを検出したいずれかの中継装置21~24は、管理装置56にアラーム情報を通知することができる。

【0045】次に、アラーム情報を受信した後の管理装置56における動作について説明する。

【0046】管理装置56は、入出力部56aを介してアラーム情報を受信すると、その内容をメモリ56cに記憶するとともにアラーム情報表示部56dによりCRT、プリンタ等の出力装置に表示させる。これにより、管理装置56が管理するネットワークシステムにおいて不正アクセスまたは障害があったことをネットワーク管理者等に知らせることができる。

【0047】また、本実施例においては、不正アクセスがあったことを知ることができるのみならず、不正アクセスをした端末装置がどの中継装置に接続されたLAN上にあるかを特定することができることを特徴とする。以下、このLANを特定する動作について説明する。

【0048】管理装置56は、受信したアラーム情報の内容からアラーム情報を発した中継装置を特定することができるので、アクセス履歴情報送信要求部56eにより前述した例においてはその中継装置21に対してアクセス履歴情報の送信要求を送る。中継装置21からアクセス履歴情報を受信すると、その内容から不正アクセスを行った端末装置54が中継装置21のポート21a

(ポート番号P1)側に存在することがわかる。逆に言うと、この時点で端末装置54がポート番号P2側に存在しないことがわかる。次に、中継装置21のポート21aにはLAN15が接続されているので、LAN15に接続されている中継装置、本実施例においては中継装置22、23、24に対してアクセス履歴情報の送信要求を送る。各中継装置22、23、24からアクセス履歴情報を受信すると、上記と同様、不正アクセスを行った端末装置54が各中継装置22、23、24のどのポート側に存在しているかを管理装置56が判定する。中継装置22、23においては、端末装置54が中継装置22、23のポート22a、23a(ポート番号P1)側に存在することがわかる。一方、中継装置24のアクセス履歴情報から端末装置54が中継装置24のポート24b(ポート番号P2)側に存在することがわかる。

【0049】以上のようにして、管理装置56は、アラーム情報とアクセス履歴情報とから不正アクセスを行った端末装置54が中継装置24のポート24bに接続されたLAN14上に存在することを特定することができる。なお、仮にLAN14に中継装置24以外の中継装置が接続され階層的なネットワーク構造になっていても上記方法を繰り返すことで不正アクセスを行った端末装置を特定することができる。この特定された内容を出力装置に表示させることで不正アクセスがあったことのみならず、中継装置から受信したアラーム情報により、どのLANに接続された端末装置からの不正アクセスであったかを特定しネットワーク管理者等に知らせることができる。

【0050】なお、中継装置の接続位置の変更、伝送媒体の接続構成の変更や増設、端末装置の接続位置変更や端末装置の活性状態変更などが発生したことをなるべく早期に自動でアクセス履歴情報に反映するために、アクセス履歴情報の保持する内容に図6に示したようにタイマカウンタを追加する方法がある。例として端末装置54から端末装置51にフレームを送信する場合の中継装置24の動作について説明するが、主要でない上記と同様の動作についての説明は省略する。なお、中継装置24には、予めアクセス履歴情報をリフレッシュするリフレッシュタイム値(しきい値)を登録しておく。

【0051】中継装置24は、アクセス履歴情報部21gに端末装置54のアドレス(Xaddr)と受信したポート番号P1を記憶する更に、端末装置54のアドレス(Xaddr)に対する記憶タイマカウンタ(Tx)を

初期値ゼロとして登録する。以降、同じフレームを同じポートから受信したときも再度端末装置54のアドレス(Xaddr)を登録し記憶タイマカウンタ(Tx)を初期値ゼロとする。一方、タイマ割り込みにより一定時間間隔毎に図7の処理がコールされる。アクセス履歴情報部21gの記憶タイマカウンタ(Ta、Tb、Th、Tm、Tx、Ty)とリフレッシュタイム値とを比較し、記憶タイマカウンタが大きければ、その記憶タイマカウンタに対応するアドレスを削除する。次に、記憶タイマカウンタに一定時間間隔にコールされる時間の相当分を加算してアクセス履歴情報の自動リフレッシュ処理を終了する。

【0052】なお、本実施例は、不正アクセスの検出について説明したが、アラーム情報を管理装置に通知する条件の設定内容により他の検出にも応用することができる。

【0053】また、本実施例は、管理装置により不正アクセスをした端末装置又は障害発生した端末装置を特定すること並びに端末装置が接続されている伝送媒体を特定することについて説明したが、一般の端末装置に管理装置56に相当する機能を有するソフトウェアをインストールすることによっても実現することができる。

【0054】

【発明の効果】以上のように、本発明によれば、中継装置は、許可/禁止情報並びにアラーム情報通知条件に基づいて不正アクセス等を検出すると、アラーム情報を管理装置に通知し、表示することができるので、ネットワーク管理者等が、不正アクセスがあったことを知ることが可能となる。

【0055】また、アラーム通知条件登録手段を設けたことにより、上記アラーム情報を管理装置に通知する条件を任意に設定することが可能となる。

【0056】また、送信要求をして得たアクセス履歴情報とアラーム情報とから不正アクセスをした端末装置を特定する手段を設けたことにより、不正アクセスがあったことを知ることができるのみならず、当該端末装置がどの伝送媒体に接続されているかを特定することが可能となる。

【0057】また、管理装置は、上記管理装置における機能を付与することで一般の端末装置においても実現可能となる。

【図面の簡単な説明】

【図1】本発明に係るセキュリティ方式が実施されるネットワークシステムの構成図である。

【図2】本実施例における中継装置の構成を示した図である。

【図3】本実施例において、各中継装置が有しているアクセス履歴情報を示した図である。

【図4】本実施例における管理装置の構成を示した図である。

【図5】本実施例における中継装置の処理を示したフローチャートである。

【図6】本実施例において、中継装置が有している記憶タイマカウンタを含むアクセス履歴情報を示した図である。

【図7】本実施例において、タイマ割り込みによりコールされる自動リフレッシュ処理を示したフローチャートである。

【図8】従来のローカルエリアネットワークシステムの構成図である。

【符号の説明】

11、12、13、14、15 LAN

21、22、23、24 中継装置

* 21a、21b ポート

21c 制御部

21d 中継制御テーブル

21e アラーム情報通知部

21f アラーム情報通知条件登録部

21g アクセス履歴情報記憶部

51、52、53、54、55 端末装置

56 管理装置

56a 入出力部

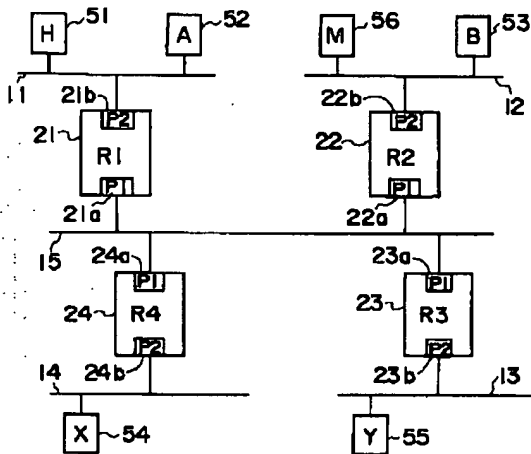
10 56b 制御部

56c メモリ

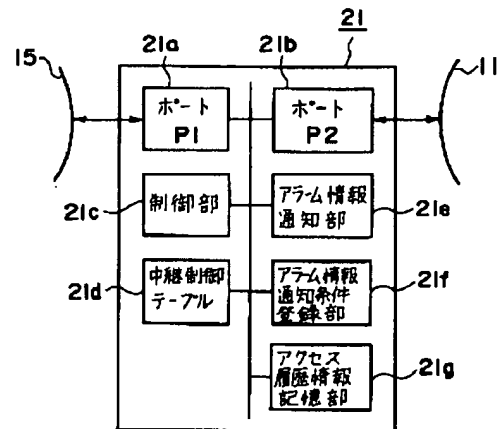
56d アラーム情報表示部

* 56e アクセス履歴情報送信要求部

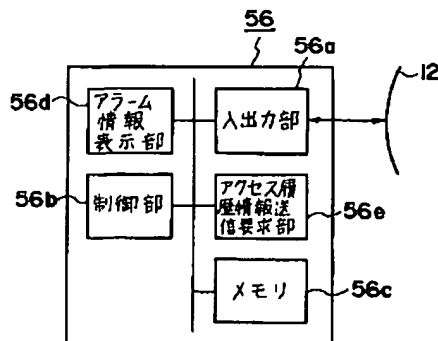
【図1】



【図2】



【図4】



【図6】

アドレス	ポート番号	記憶タイマカウンタ
A-adr	P1	Ta
B-adr	P1	Tb
H-adr	P1	Th
M-adr	P1	Tm
X-adr	P2	Tx
Y-adr	P1	Ty

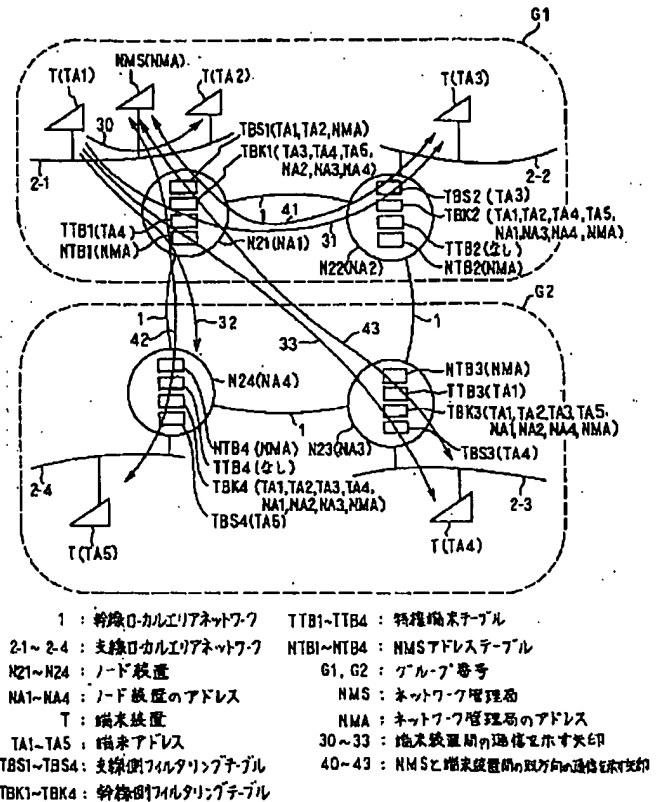
【図3】

R1のアクセス履歴		R2のアクセス履歴	
アドレス	ポート番号	アドレス	ポート番号
A_addr	P2	A_addr	P1
B_addr	P1	B_addr	P2
H_addr	P2	H_addr	P1
M_addr	P1	M_addr	P2
X_addr	P1	X_addr	P1
Y_addr	P1	Y_addr	P1

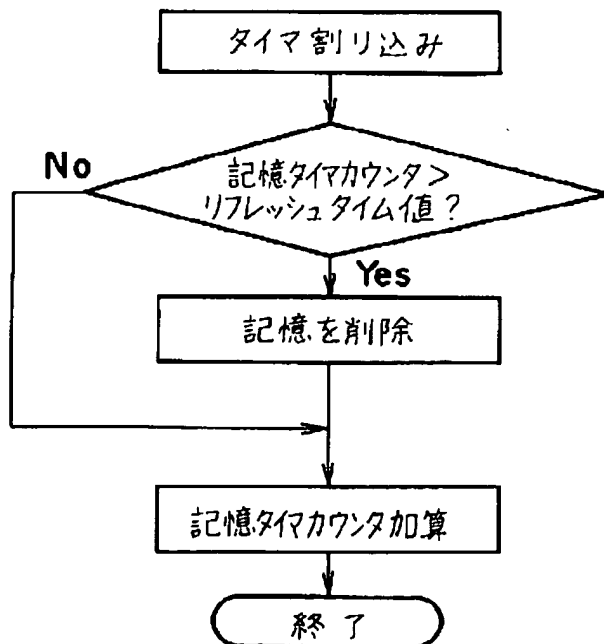
R3のアクセス履歴		R4のアクセス履歴	
アドレス	ポート番号	アドレス	ポート番号
A_addr	P1	A_addr	P1
B_addr	P1	B_addr	P1
H_addr	P1	H_addr	P1
M_addr	P1	M_addr	P1
X_addr	P1	X_addr	P2
Y_addr	P2	Y_addr	P1

A_addr : 端末装置Aのアドレス
 B_addr : 端末装置Bのアドレス
 H_addr : 端末装置Hのアドレス
 M_addr : 端末装置Mのアドレス
 X_addr : 端末装置Xのアドレス
 Y_addr : 端末装置Yのアドレス

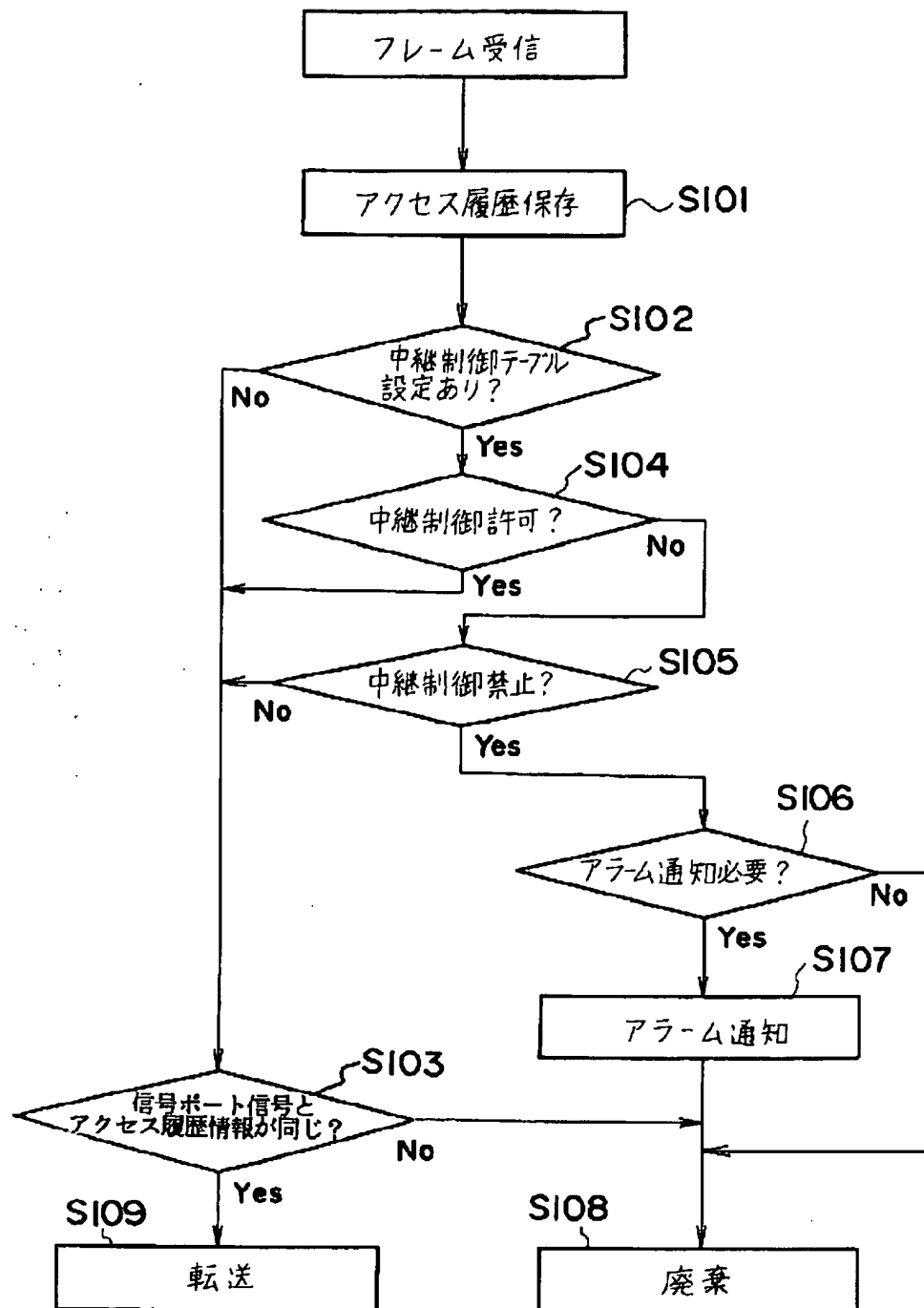
【図8】



【図7】



【図 5】



フロントページの続き

(51)Int.Cl.⁶

G 0 6 F 13/00

15/00

H 0 4 L 12/40

識別記号

3 5 1 Z 7368-5B

3 3 0 A 7459-5L

庁内整理番号

F I

技術表示箇所